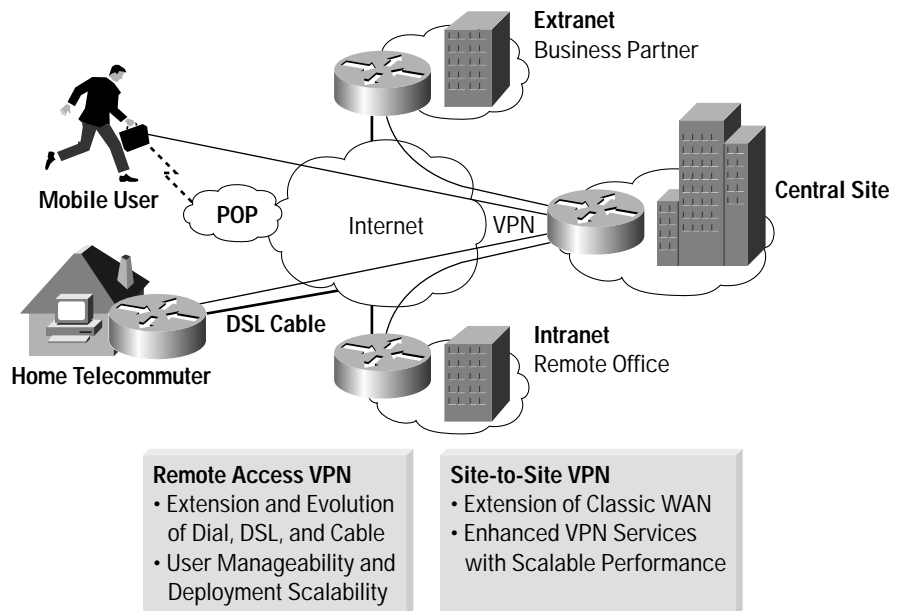


# Cisco Managed IPsec Customer Premises Equipment Virtual Private Network Solution

## Executive Summary

This document provides a technical perspective of the Cisco Managed IP Security (IPsec) Customer Premises Equipment (CPE) Virtual Private Network (VPN) solution. A service provider can employ this solution to centralize and speed up provisioning, deploy bundled end-to-end VPN services, and generate new revenue streams from the expanded offerings. The Cisco IPsec CPE VPN solution can be deployed over an existing IP infrastructure without any network upgrades or changes to the network core. By deploying this scalable solution that includes IPsec-enabled CPE and the Cisco VPN Solution Center (VPNSC) for centralized provisioning, service providers can strengthen customer loyalty, introduce greater service differentiation, and expand overall market opportunities. (See Figure 1.)

Figure 1  
 Remote Access and Site-to-Site VPNs





## IPSec CPE VPN Summary

IPSec protocol, a framework of open standards, provides data confidentiality, data integrity, and data authentication over unprotected networks such as the Internet. At the IP layer, IPSec provides secure tunnels and serves to protect and authenticate IP packets between participating IPSec devices (peers) such as Cisco PIX<sup>®</sup> Firewall units, VPN clients, and VPN-enabled routers. IPSec can provide any combination of the following network security services:

- *Data confidentiality*—Packets can be encrypted before transmission.
- *Data integrity*—Packets are authenticated to ensure that the data has not been altered during transmission.
- *Data origin authentication*—The source of received packets can also be authenticated. (This service is dependent upon the data integrity service.)
- *Antireplay*—Old or duplicate packets can be detected and rejected to avoid replay attacks.

IPSec allows network managers to designate the packets of those sessions that should be sent through secure tunnels, and to define the parameters that should be used to protect sensitive packets. When a sensitive transmission begins, an appropriate secure tunnel is established and the packets are sent through the tunnel to the destination.

Using these secure tunnels, the IPSec standard includes the procedures and encryption methods for handling sensitive transmissions. Multiple IPSec tunnels can exist between two points to secure different sessions, with each tunnel using different security methods. For example, one session might require only authentication of the sender, whereas other sessions call for encrypting transmitted data as well as authenticating the sender.

Network architecture flexibility and ubiquity uniquely position Cisco to supply IPSec VPN technology and solutions to service providers. Existing Cisco networking products—routers, WAN switches, access servers, and firewalls—ensure the smooth deployment of VPN services into customer networks. The proliferation of Cisco equipment in existing service provider IP, Frame Relay, and ATM backbones provides a high degree of feature integration over the WAN, including common bandwidth management and quality-of-service (QoS) functions for both service provider and enterprise networks. The strong base of existing Cisco equipment in service provider and enterprise networks simplifies the deployment of VPN services and further strengthens the integration of provider and enterprise networks.

### **Solution Benefits**

The Cisco solution provides:

- *Improved time to market*—The Cisco solution is centralized and, therefore, simplifies the otherwise time-consuming provisioning process compared to distributed management solutions. Cisco IPSec CPE VPN solutions lead to services that can be turned on in hours instead of days or weeks.
- *Reduced operational costs*—Costs are lowered by centralized network and service management processes.
- *Reduced total cost of ownership*—Instead of developing custom management solutions, service providers can use the Cisco Managed IPSec CPE VPN integrated management solution in a standalone mode or integrated with a service provider's existing operations-support-system (OSS) environment.
- *Consistency and simplicity of VPN service management*—The Cisco offering enables the management of firewall, VPN, and routing services in one integrated solution, reducing costs and simplifying administration for the service provider.



## Provisioning

The Cisco Managed IPsec CPE VPN solution provisions VPNs in full-mesh, partial-mesh, or hub-and-spoke topologies. It supports both IPsec and IPsec-over-generic routing encapsulation (GRE) tunneling. A VPN service can be augmented by provisioning subtopologies between CPE devices, each associated with a separate or consistent policy.

Provisioning can be performed using a graphical user interface (GUI), or Common Object Request Broker Architecture (CORBA) application programming interfaces (APIs). The GUI approach simplifies the process of entering VPN service request information, including customer and service-level agreement (SLA) profiles. When entered, the Cisco solution uses this information to automatically update configurations on the associated devices. Services can be activated immediately or at a scheduled time. When activated, a just-in-time (JIT) provisioning process uploads the current network configuration from the associated devices, creates Cisco IOS<sup>®</sup> configuration instructions, and downloads the instructions back to the devices. By uploading the current configuration, the Cisco solution can accurately generate the minimized set of commands required, and can also validate the operator's entries to identify any conflicts with the current configuration. The Cisco solution tracks the current state, including error conditions, of the service request and scheduled tasks.

The Cisco Managed IPsec CPE VPN solution includes a template provisioning system (TPS) for fast, flexible, and extensible Cisco IOS command generation. Standard templates can be used to generate configlets for common provisioning tasks. Using the GUI, users can modify these templates or generate custom templates for streamlining tasks unique to a particular environment or service.

## Auditing

When a service is provisioned, the Cisco solution collects a variety of data from related network elements to determine and track the state of the active services. Router configuration files are regularly uploaded and analyzed. The information gathered is used to update the status of service requests, add to the service request history, and generate status reports. Audits can be requested or scheduled using the GUI or API.

## SLA Monitoring

SLAs are monitored for round-trip times, availability, and threshold violations between VPN devices. The performance data is collected using the Cisco IOS Service Assurance Agent (SAA). Formerly called the Response Time Reporter, the Cisco SAA is based on the round-trip time monitoring (RTTMON) Management Information Base (MIB). The Cisco IPsec CPE VPN solution can create a variety of SAA probes or SLA definitions using the SAA MIBs. SAA probes can automatically be provisioned along with the VPN services. Various SAA probe parameters can be configured when creating the probe.

When SAA probes are configured, the Cisco solution collects SAA data regularly from these probes and can output this data to a customer's report-generation software for generating hourly, daily, monthly, and annual reports. Thresholds can be set for the types of data collected, and the reports will note any violations. For monitoring SLAs in real time, SAA probes can be configured to forward events to the appropriate OSS when a threshold is crossed. Third-party applications can be used to handle such events. The Cisco solution can also collect and report on performance data collected from the committed-access-rate (CAR) MIB.



## High Availability

For high availability of provisioning, the Cisco VPNSC can integrate Sun Clustering so that workstations are protected with automatic failover capability. This optional capability also provides database journaling and replay in the event of a server failure, and includes repository administration tools to control database size and backup.

## Assumptions

The Cisco Managed IPSec CPE VPN solution enables service providers to offer managed VPN services over existing networks to enterprise or small and medium-size business customers. This solution does not require Multiprotocol Label Switching (MPLS) or any changes to the service provider's core network. Instead, core routers simply forward plain IP packets.

## Deployment Model

IPSec tunnels or IPSec-over-GRE tunnels can be provisioned using full-mesh, hub-and-spoke, or partial-mesh topologies. All tunnels overlay the core network to provide site-to-site VPN connectivity. Figure 2 shows a VPN with full-mesh (or any-to-any) connectivity between sites. Figure 3 shows the hub-and-spoke VPN topology, which allows spoke sites to talk directly to a central hub for simplified scaling compared to the full-mesh network design. When provisioning IPSec tunnels, spokes generally have connectivity to hubs but not to other spokes. When using IPSec-over-GRE tunnels, spoke sites may have routing connectivity through the hub site.

Figure 2  
Full-Mesh Topology for IPSec or IPSec-over-GRE Tunnels

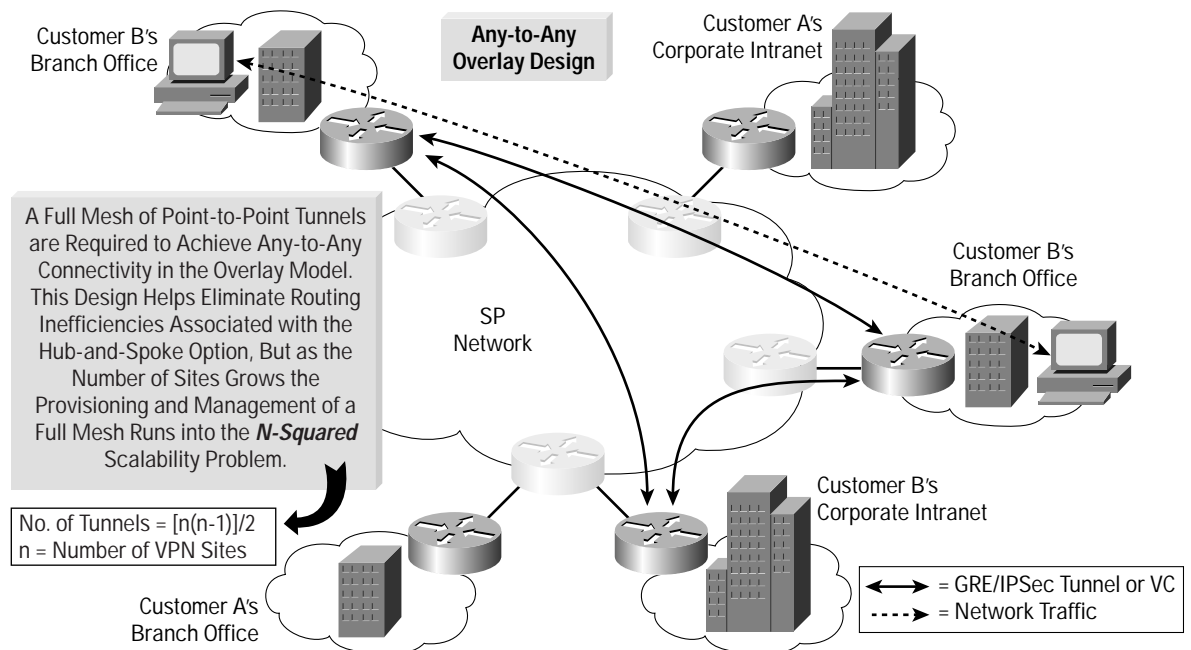






Figure 4  
Intranet VPN Using IPSec or IPSec-over-GRE Tunnels Between Customer Sites

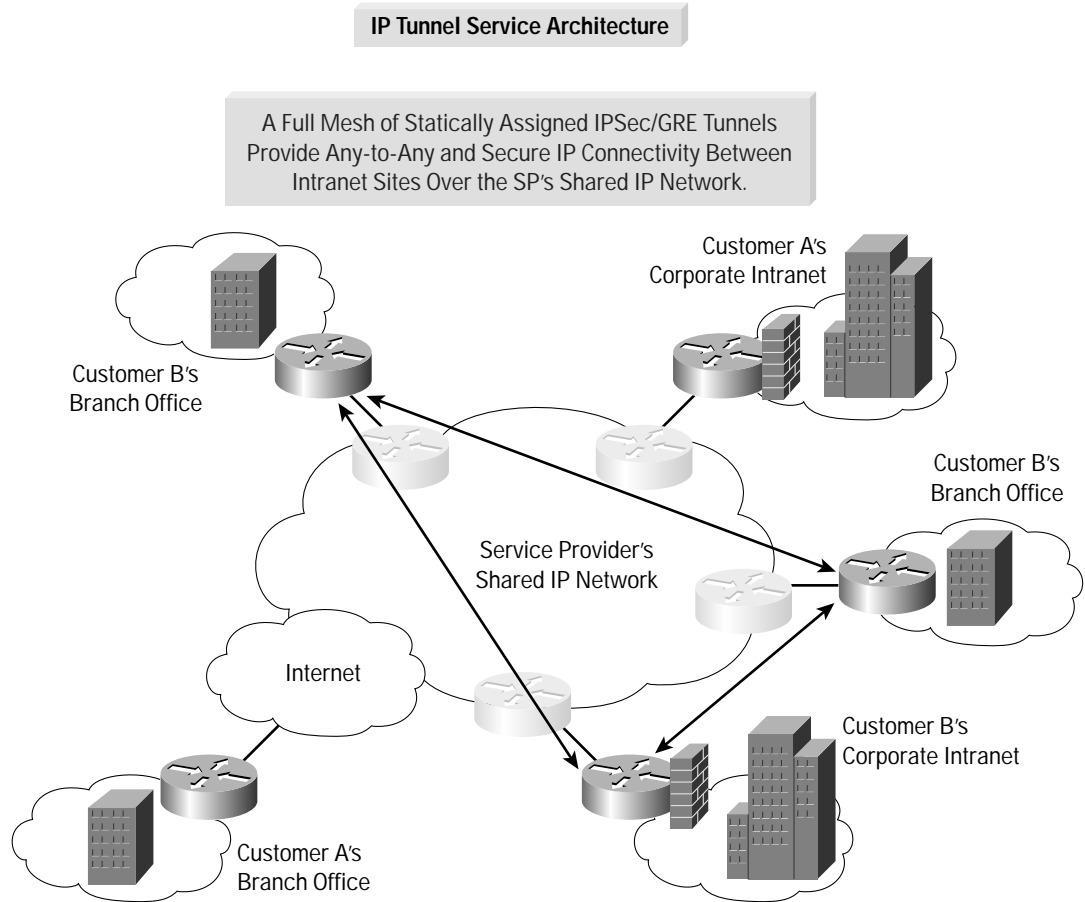
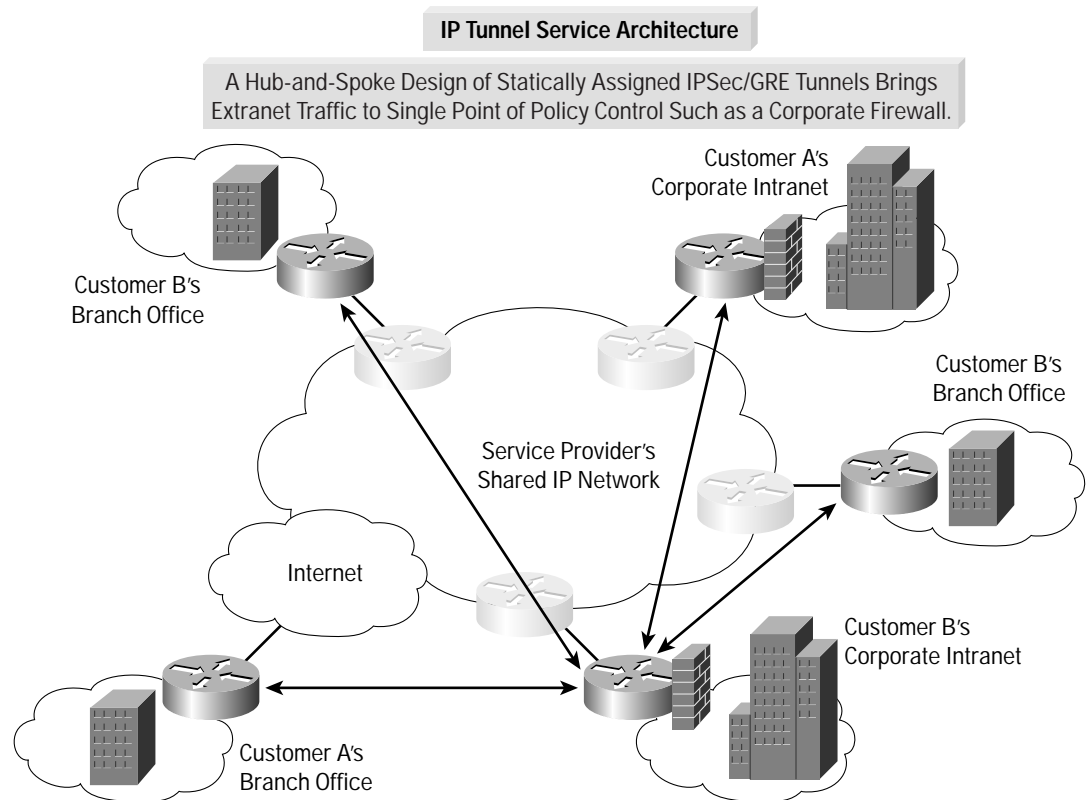




Figure 5  
Extranet VPN Using IPSec or IPSec-over-GRE Tunnels Between Customer Sites



## Cisco IPSec CPE VPN Solution Components

### CPE Equipment

Cisco IPSec CPE VPN solutions offer end users a choice of the following CPE:

- Cisco 800 Series routers
- Cisco uBR900 Series cable routers
- Cisco 1700 Series routers
- Cisco 2600 and 3600 series routers
- Cisco 7100 and 7200 series routers

### Cisco VPNSC

The Cisco VPNSC management platform serves as an effective and efficient solution for provisioning, service auditing, SLA and performance monitoring, accounting, and usage collection for VPN services. Data can also be provided for billing and report generation. The Cisco VPNSC Software validates syntax and integrity to ensure accuracy and network stability and to identify inconsistencies in the configuration files before they are deployed to the live network.

## Cisco Provisioning Center

The Cisco Provisioning Center integrates with the Cisco VPNSC to add flow-through provisioning capabilities for environments that require support for multiplayer or multivendor topologies.

## Cisco Info Center

The Cisco Info Center can also be combined with the Cisco VPNSC to monitor network performance and faults from a service-oriented perspective. The provided capabilities include correlation and filtering, monitoring, customer and administrative partitioning, and flow-through integration to other systems.

## Cisco IOS Release 12.2.1M or Higher

Common Cisco IOS Software spanning the CPE and service provider network makes it possible to transparently integrate the end user and corporate networks.

For More Information

For more information about Cisco VPN solutions, go to:

<http://www.cisco.com/go/vpnsolutions>



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0301R) SP/LW4085 02/03